Secure Software Development

Agenda

I. About NIC MX
II. Introduction
III. Securing Code/Data
IV. Securing Passwords
I. About Us

- ccTLD for Mexico, part of LACNIC
- More than 130 employees
- ~700,000 .MX domain names (2014)

<table>
<thead>
<tr>
<th>Statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>.com.mx</td>
<td>442,228</td>
</tr>
<tr>
<td>.gob.mx</td>
<td>7,404</td>
</tr>
<tr>
<td>.net.mx</td>
<td>362</td>
</tr>
<tr>
<td>.edu.mx</td>
<td>9,724</td>
</tr>
<tr>
<td>.org.mx</td>
<td>19,130</td>
</tr>
<tr>
<td>.mx</td>
<td>227,708</td>
</tr>
<tr>
<td>TOTAL</td>
<td>706,556</td>
</tr>
</tbody>
</table>
II. Introduction

- In-house Applications

- DNS Master Database

- Security application

- Epp from registrars

- Intranets

- Extranets

- Internal applications

- DNS Master

- DNS slave
II. Introduction

• Different environments with same configurations...

Development

~40 apps

~30 people devs/testers

Production

~120 app instances

Redundant
- Apps
- Servers
- Devices
- Datacenters

scalability
Possible **Risks**...

- Code Leaks
- **Unauthorized access** to Sensitive Data from Development environment
- Compromised **passwords**
II. Introduction

**Measures to...**

- Secure code
- Secure data
- Secure passwords
II. Securing Code/Data

Isolated servers...

...with copy restrictions
II. Securing Code/Data

1. VPN Access

- from Inside
- from Outside

DEV Servers
II. Securing Code/Data

2. Separated network segments
II. Securing Code/Data

3. Firewall access

- Only Remote Connections Allowed
II. Securing Code/Data

Dummy Data in...

Production

Development

Periodic refresh of data

John Smith
811-57-891

Dummy Dummy
II. Securing Code/Data

Advantages

• Code is safe from being copied.
• Data is protected.
• Access controlled to resources.
III. Securing passwords

When applications need access to resources...

- Database Passwords
- Certificate phrases
- Password for provider’s services
- etc
III. Securing passwords

How an application gets its credentials?

1° Config. File
- Starts fast
- Easy to steal

2° Encrypted & Ask for creds
- Hard to steal
- Hard to admin (many servers)

3° Centralized app
- Hard to steal
- Easy to admin
- One point of failure
III. Securing passwords
CIS (Credential Information Service) provides credentials to applications. However, it doesn’t store passwords.
III. Securing passwords

Credentials are stored encrypted in another database

CIS just decrypts them

Master key
III. Securing passwords

A Master Phrase must be typed by an Administrator when CIS starts...

...and It remains loaded in Memory
III. Securing passwords

CIS can serve many credentials...

...to many applications.

Protected
Master key

Encrypted credentials
III. Securing passwords

What if a **credential** is compromised...?

...only that credential needs to be changed
III. Securing passwords

What if master phrase is compromised...?

...all credentials and master key must be changed.
III. Securing passwords

Advantages

- Only one point of failure
- Nobody knows passwords
- Easy to change passwords if someone leaves or a credential is compromised
Questions?

Thank you!

Carlos Cardenas